

MEMORANDUM

TO: Federal Communications Commission

FROM: Myung A. Kim (7781245)

DATE: April 27, 2006

SUBJECT: Protection of Customer Proprietary Network Information (CPNI)

QUESTIONS PRESENTED

The following issues are presented for resolution: (1) whether telecommunications carriers have taken adequate measures to protect the privacy of customer proprietary network information (“CPNI”); and (2) what additional steps, if any, should be taken to further protect the CPNI.

STATEMENT OF FACTS

CPNI is the data collected by telecommunications corporations about a consumer's telephone calls. It includes the time, date, duration and destination number of each call, the type of a customer's network subscription, and other information that appears on the consumer's telephone bill.¹ Due to the personal nature of the information, the privacy of an

¹ FCC Notice of Proposed Rulemaking In the Matter of Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Petition for Rulemaking to

individual is directly implicated and disclosure of the information to third parties violates a number of statutes including the 1996 Telecommunications Act. Congress enacted the Telecommunications Act of 1996² to stimulate competition in telecommunication services while protecting the privacy of consumers. It however placed fewer restrictions on the dissemination of information that is not highly sensitive than on the dissemination of more sensitive information the carriers has gathered about particular customer. Congress categorized CPNI as highly sensitive and accorded CPNI the category of customer information the greatest level of protection.³

A deeply rooted principle of American law is that individual privacy is a fundamental value to be protected and that consumers should be guarded from the harms that can arise from others obtaining their private information for improper purposes.⁴ The release of the information without a consumer's knowledge can lead to identity theft, fraud, harm to personal safety. In *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003), the New Hampshire Supreme Court held that information brokers and private investigators could be liable for the harms caused by selling personal

Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information (posted February 14, 2006). Available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-10A1.doc

² 47 U.S.C. § 222 *et. seq*

³ 47 U.S.C. §222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information. §222(b) states that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may only use such information for that purpose and not for its own marketing efforts. §222(c) outlines the confidentiality protections applicable to customer information.

⁴ the Supreme Court has found that the U.S. constitution contains "penumbras" that implicitly grant a right to privacy against government intrusion. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

information. In that case, a stalker obtained a young woman's personal information, including her Social Security number and employment information from an internet-based information service company before he located and shot her to death.

Against this backdrop, the importance of the current debate on CPNI protection cannot be overemphasized. On one end of the spectrum, privacy advocates such as the Electronic Privacy Information Center (“EPIC”) states that the existing security and authentication standards for access to CPNI are inadequate and that significant privacy violations that have occurred as a result.⁵ In response, telecommunications carriers contend that the petition must be denied because the existing measures and legislation provide sufficient protection for CPNI. Based on these facts, Section I of this commentary analyzes the information provided by the opposing sides, namely, the nature and the extent of the problem. Despite telecommunications carriers assertion that they have sufficient measures to prevent violation of consumer privacy, facts indicate that in the past CPNI has been stolen and sold for improper purposes systematically. Section II concludes with policy recommendations.

DISCUSSION

I. Nature and Scope of the Problem:

⁵ Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 95-115 (filed Aug. 30, 2005).

A. Petition by the Electronic Privacy Information Center

Under the current system, data brokers and private investigators take advantage of telecommunications carriers' inadequate security by pretending to have authority to access protected records and by cracking consumers' online accounts with the carriers.⁶

For example, Intelligent e-Commerce, Inc. ("IEI"), a company that runs the online investigation website bestpeoplesearch.com, provides detailed call records for the past 100 calls of either a business or residential phone line if the requestor provides the telephone number, and address of the account holder.⁷

EPIC raises the concern that the information can be accessed by illegal means.⁸ On its public website, for instance, IEI appears to be aware of the potential harm that can result from providing information, as it attempts to disclaim a wide variety of harms in its Terms and Conditions.⁹ The terms on the site require that the requestor take the pledge that the request does not involve any "intention to harm, to cause harm, to harass, to stalk (as

⁶ Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wpdyn/content/article/2005/07/07/AR2005070701862_pf.html.

⁷ On January 18, 2006, the president of IEI made a press release stating that "in light of the recent activities of its competitor's, [IEI] has decided to voluntarily cease offering call records from its web sites. IEI concluded that continuing to provide the service would link it to disreputable companies who do not use any safeguards to protect against the potential dangers of this service. Available at <http://www.prweb.com/releases/2006/1/prweb334327.htm> .

⁸ *Id.*

⁹ Petition for rulemaking at 17.

described by applicable laws), or to otherwise take any illegal or proscribed action against any person or entity."¹⁰ IEI also requires information requestors to indemnify the company from harms flowing from the use of personal data.¹¹ The problem here is that such measures are hardly adequate to prevent harm or to make its actions legal. Even though IEI asserts that they obtain information through private investigators, private investigators do not have special rights to solicit others to violate the law with impunity.¹²

Consequently, the problem raised by the example is three-fold: First, since the information is stolen and sold surreptitiously, consumers have so little control over their CPNI even though so much is at stake. Unlike cases involving tangible goods, the illegal dissemination of CPNI would almost always cause an irreparable harm even if the information could be recovered later. Second, as the IEI's illegal online business indicates, at least some telecommunications carriers have failed to provide adequate protection over CPNI. With proper safeguards to prevent stealing and dissemination, the information would not have been available to illegal information brokers in the first place.¹³ There are loopholes in the security measures that make illegitimate practices of online data brokers possible. Finally, the illegal

¹⁰ *Id.* Attachment C

¹¹ *Id.*

¹² Private investigators are regulated by a wide range of state laws, i.e., licensing requirements ranging from payment of a licensing fee to extensive occupational training and experience. However, none gives private investigators special rights to solicit others to violate the law. See Ala. Code § 40-12-93; 12 Cal. Bus. & Prof. Code § 7541.

¹³ IEI has been offering, for example, the "Residential Local/LATA Phone Records" for \$87 to those who wish to purchase a copy of a third party's residential long distance bill for the last billing cycle

activities do not appear to be random or isolated events. In addition to IEI, there are various sites providing on line investigation services and offering CPNI for value.¹⁴ For instance, a search in the Google search engine returns many sites, both as sponsored links and as normal search results of online investigator sites similar to bestpeoplesearch.com. Many of these sites offer sales to the general public.¹⁵

B. Response by Telecommunications Carriers

The telecommunications carriers oppose the EPIC petition, stating that they have adequate measures to protect CPNI and that existing legislation and rules create sufficient safeguards.¹⁶ Moreover, they assert that additional rules aimed at CPNI should be avoided because they will impose unnecessary additional burdens on carriers. They provide the following arguments in support of their claim:

The Existing CPNI Practices Are Adequate:

¹⁴ Petition for rulemaking, Attachment C.

¹⁵ Abika.com offers call detail¹⁶ and the actual identity of people who use screen names on AOL, Match.com, Kiss.com, Lavalife, and Friendfinder.com. Peoplesearchamerica.com offers call detail¹⁸ and P.O. Box records. Onlinepi.com offers cell phone location information. Discreetresearch.com offers call detail. Datatraceusa.com offers call detail.

¹⁶ The Wireless Association Comments in Opposition to EPIC Petition for Rulemaking, Oct. 31, 2005

The telecommunications carriers allege that existing regulations over CPNI are adequate. They cite Section 222 of Title 47 and the Commission's implementing rules which provide "every telecommunications carrier has a duty to protect the confidentiality of proprietary information," and state that every telecommunications carrier takes that responsibility seriously.¹⁷ The telecommunications carriers also argue all public companies must meet the requirements of the Sarbanes-Oxley Act ("SOX"),¹⁸ which requires the adoption and implementation of policies and operational controls that address material risk. Finally, they state that carriers under the existing scheme are only permitted to disclose CPNI in a limited number of circumstances (i.e., disclosure only after the customer gives written authorization).

This line of argument is not persuasive because it does not adequately address the issue at hand. There have been a number of violations of the existing rules which raised doubts about the carriers' ability to detect and prevent such violations. The telecommunications carriers merely state that there are sufficient measures to protect CPNI,

¹⁷ *Id* at 6.

¹⁸ Under the Sarbanes-Oxley Act, 15 U.S.C. § 7241, public companies must have their signing officers, usually CEOs and CFOs, certify personally that they are responsible for establishing and maintaining internal controls for accurate financial statements and that they have designed such internal controls. Similarly in the context of CPNI protection, the current FCC rules require that telecommunications carriers have an officer to sign a compliance certificate stating that they have adequate operating procedures to protect CPNI. However, there has been a lack of uniformity relating to the certification process. More facts interwoven in the discussion, beginning *infra* at 9.

but they do not clearly state how they are enforced. Thus, they have not addressed the issue adequately.

Keeping Promises to Customers:

The carriers also state that they subscribe to CTIA's Consumer Code for Wireless Service, which requires the participating carrier to adopt and publish a privacy policy that explains its information practices to customers.¹⁹ The "promise" is that the consumer's information is being fully protected. This argument is unavailing. In December of 2005, for instance, the New York Times revealed that the government had instituted a comprehensive and warrant-less electronic surveillance program that ignored the careful safeguards set forth by Congress.²⁰ This surveillance program, purportedly authorized by the President at least as early as 2001 and technically assisted by telecommunications carriers, intercepted and analyzed the communications of ordinary citizens in the U.S. Recently, the Electronic Frontier Foundation (EFF) filed a class-action lawsuit against AT&T on January 31, 2006, accusing the company of violating the privacy of its customers by collaborating with the National Security Agency (NSA) in its

¹⁹ Comments of SBC Communications Inc. Docket No. 96-115 (filed October 31, 2005); The Wireless Association Comments in Opposition to EPIC Petition for Rulemaking, Docket No. 96-115 (filed October 31, 2005).

²⁰ James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, December 16, 2005, at A 1.

illegal program to wiretap without warrants.²¹ It may be true that a material difference exists between selling CPNI and complying with a federal officer's demand. Nevertheless, these examples show that some telecommunications carriers have not been completely forthright about the facts related to CPNI.

Argument 3: Adequate Information and Education for Consumers to Protect Their Privacy.

The telecommunications carriers also advise customers about how to protect their CPNI, telling them “before discarding [customer’s] phone or PDA, trading it in or giving it away, be sure to remove and retain SIM card and follow the manufacturer's instructions for deleting all personal information on the device itself.”²² This again is a moot point in the context of the discussion at hand. As a general rule, consumers should exercise due care in protecting their privacy. However, the concern here is whether the telecommunications carriers are fulfilling their own obligation to prevent illegal sources from violating their consumer privacy.

II. Recommendations & Conclusion

Under the Communications Act of 1934, the FCC was authorized to make rules and regulations to ... “[from time to time, as public convenience,

²¹ Information about the class action available at <http://www.eff.org/legal/cases/att/>

²² The Wireless Association Comments at 14.

interest, or necessity required].”²³ Additionally, the FCC has ancillary authority to perform any acts and make such rules and regulations as may be necessary in the execution of its functions.²⁴ Here, the FCC should exercise its authority to protect consumer privacy since the violation directly implicates public interest and safety. A clear set of rules and regulations for telecommunications carriers will increase their efforts to further protect CPNI and thus the public interest in preserving consumer privacy. Consequently, the FCC should favorably consider the following measures recommended by EPIC.

Certification and Criminal Sanctions

Under the Sarbanes-Oxley Act, corporations have been held to strict standards of transparency so as to deter illegal insider trading and fraudulent activities.²⁵ Similar principles should apply here. Currently, the FCC rules require each telecommunications carrier to have an officer as an agent of the carrier to sign a compliance certificate stating that the company has adequate operating procedures and to avail that certification to the public.²⁶ However, there has been a lack of uniformity to the certification process and deadlines, which created confusion and prevented effective

²³ 47 U.S.C. § 151.

²⁴ 47 USC § 153(33): “transmission ... including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission”.

²⁵ 15 U.S.C. § 7241, et seq.

²⁶ 47 C.F.R. § 64.2009(e); CPNI Order, 13 FCC Red at 8199.

enforcement of the existing rules.²⁷ The FCC should amend the rules to require all telecommunications carriers to comply with uniform certification procedural rules. It should also require telecommunications carriers to provide an explanation of any actions against data brokers and summary of all consumer complaints received in the past year concerning the unauthorized release of CPNI. Any violation of these procedural requirements or misrepresentation of facts should be punishable by criminal sanctions and heavy fines. This will deter illegal activities by raising the cost of wrongdoing and give incentives to telecommunications carriers to make considerable efforts to protect CPNI.

Unique Passwords

Unique passwords for access to account information would greatly increase security. Many carriers already have the capacity to offer online access to customer accounts as a customer service, and a personally selected password to account information will give more autonomy to consumers to control access to their CPNI. Telecommunications carriers have opposed this suggestion stating that carriers already receive a larger number of requests for password assistance from consumers who claim that they have forgotten the key.²⁸ They claim that creating an extra password will only increase the chance of consumers misplacing the access key and thereby exposing their private information to wrongdoers. By implication, the carriers are also

²⁷ FCC Notice of Proposed Rulemaking In the Matter of Implementation of the Telecommunications Act of 1996 at 12.

²⁸ *Id.* at 21.

concerned about the extra costs and time associated with creating and maintaining the passwords. However, the potential harm does not outweigh the benefits. When consumers claim that they have lost passwords, carriers could prevent security problems by using an extra degree of caution and providing the passwords only to the email address of the subscribers.

Audit Trails

EPIC calls for audit trails regarding access to CPNI. In response, telecommunications carriers contend that such procedures already exists and that an audit trail that provides a record of a disclosure is useful only when someone complains about or reports a violation.²⁹ As a matter of fact, the evidence presented by EPIC regarding on-line brokers' illegal activities as well as the civil litigation by EFF indicate that such complaints are already in existence. More complaints will be forthcoming if information regarding surreptitious dissemination of CPNI becomes available to those who are affected.

Encryption

EPIC also calls for encryption of calling records in storage. The threat of disclosure is from various forces. It appears that the

²⁹ *Id.* at 22.

information can be disseminated from within, by voluntary disclosure by the telecommunications carriers (or their employees), and from outside forces such as hackers or person who claim to be the customer. Imposing such an encryption requirement on carriers will raise the level of security for consumers.

Notice

In July 2003, California Senate Bill 1386 went into effect, becoming the first law in the Nation to establish notification requirements regarding security breaches that involve the compromise of personal information. Since that time, twenty more states have passed similar legislation, and Congress is considering enacting a uniform federal security breach notification statute. Under this legislative structure, notification of affected consumers should be required for unauthorized disclosure of personal information such as disclosure of CPNI to incorrect or unauthorized recipients.

Conclusion:

EPIC has expressed legitimate concerns about consumer privacy. Yet the telecommunications carriers' responses are far from being satisfactory. In their commentaries, the carriers state that they have sufficient security measures but fail to explain the extent to which those measures are enforced. Considering the seriousness of the harm that can be caused by illegal usage of CPNI and the broad implication it has on the individual right to privacy,

the Commission should carefully review the evidence provided by EPIC and rule in its favor.